USA
Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

Information services, finance, and public administration sectors are the most targeted industries, both in phishing and dark web threats.

Selling and sharing stolen data dominate dark web forums, representing over 93% of activities, signaling an active criminal marketplace.

Data and unauthorized access are the top commodities, with 57.46% of dark web posts related to stolen databases.

RansomHub, PLAY Ransomware, and Akira are leading ransomware groups targeting the US, but a diverse set of other actors make up the majority.

Phishing attacks heavily target the Crypto/NFT, information services, and public sector, leveraging fake pages that increasingly use HTTPS (76.4%) to appear legitimate.

Stealer logs show massive credential exposure, with over 630,000 email/password pairs leaked, alongside credit card data and victim IP addresses.

Popular domains compromised include Reddit, Bing, Instagram, Facebook, and Amazon, highlighting the targeting of mainstream platforms.

Technical Details

This report based on data collected between April 2024 and March 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around the US.

In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting the US, their detailed profiles and the necessary data that summarizes the ransomware activities.

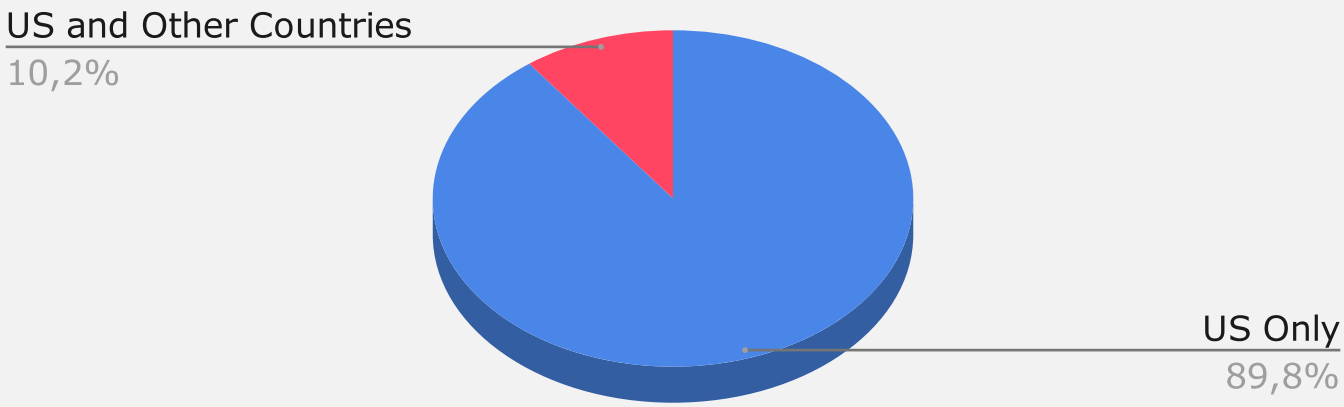
Stealer Logs Statistics chapter is all about stealer malware and the data around leaked credentials. These days, hackers don't hack, they log in. It is important to make sure that employee credentials are not compromised.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.

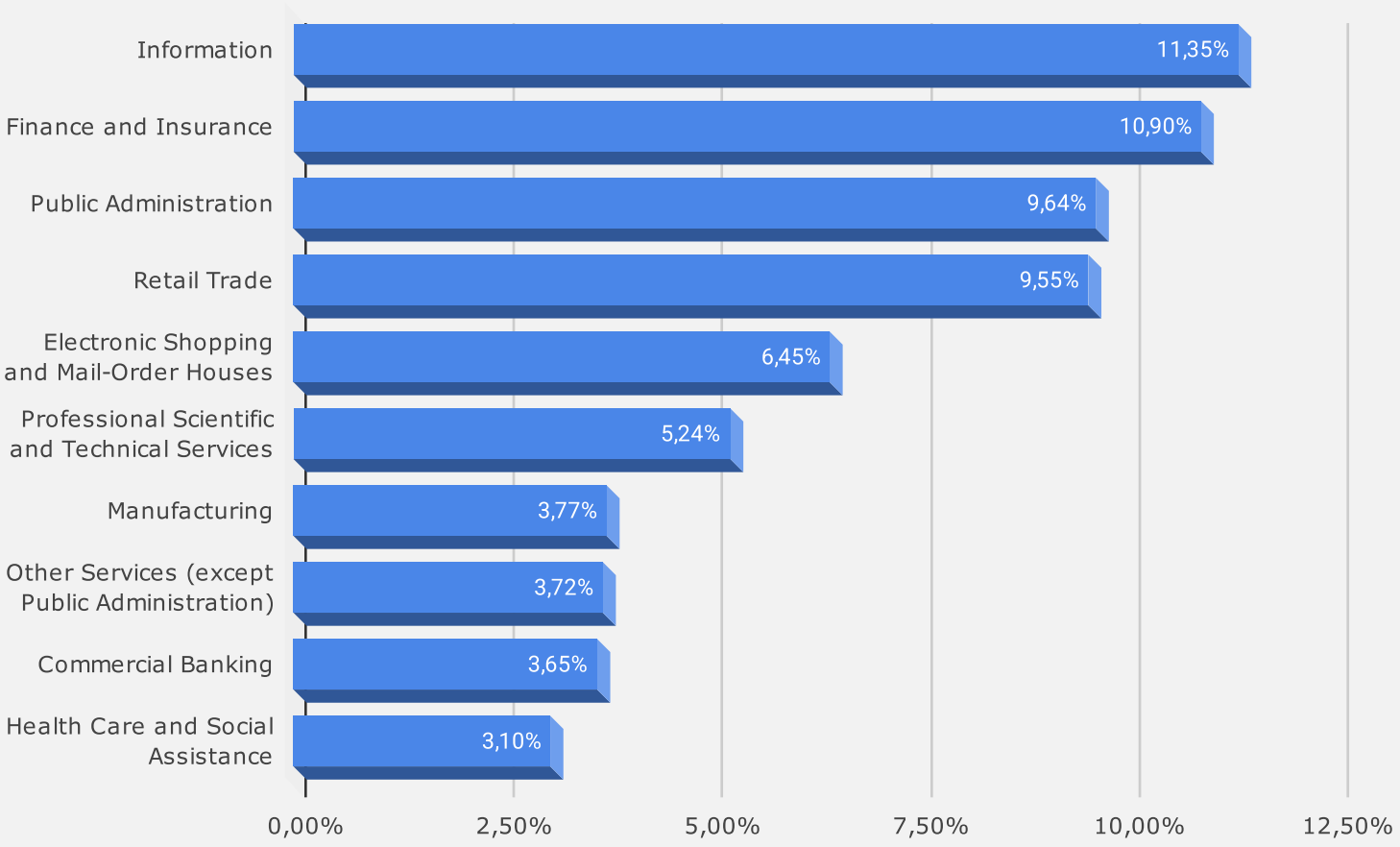
Dark Web Threats

Distribution of Dark Web Threats by Country



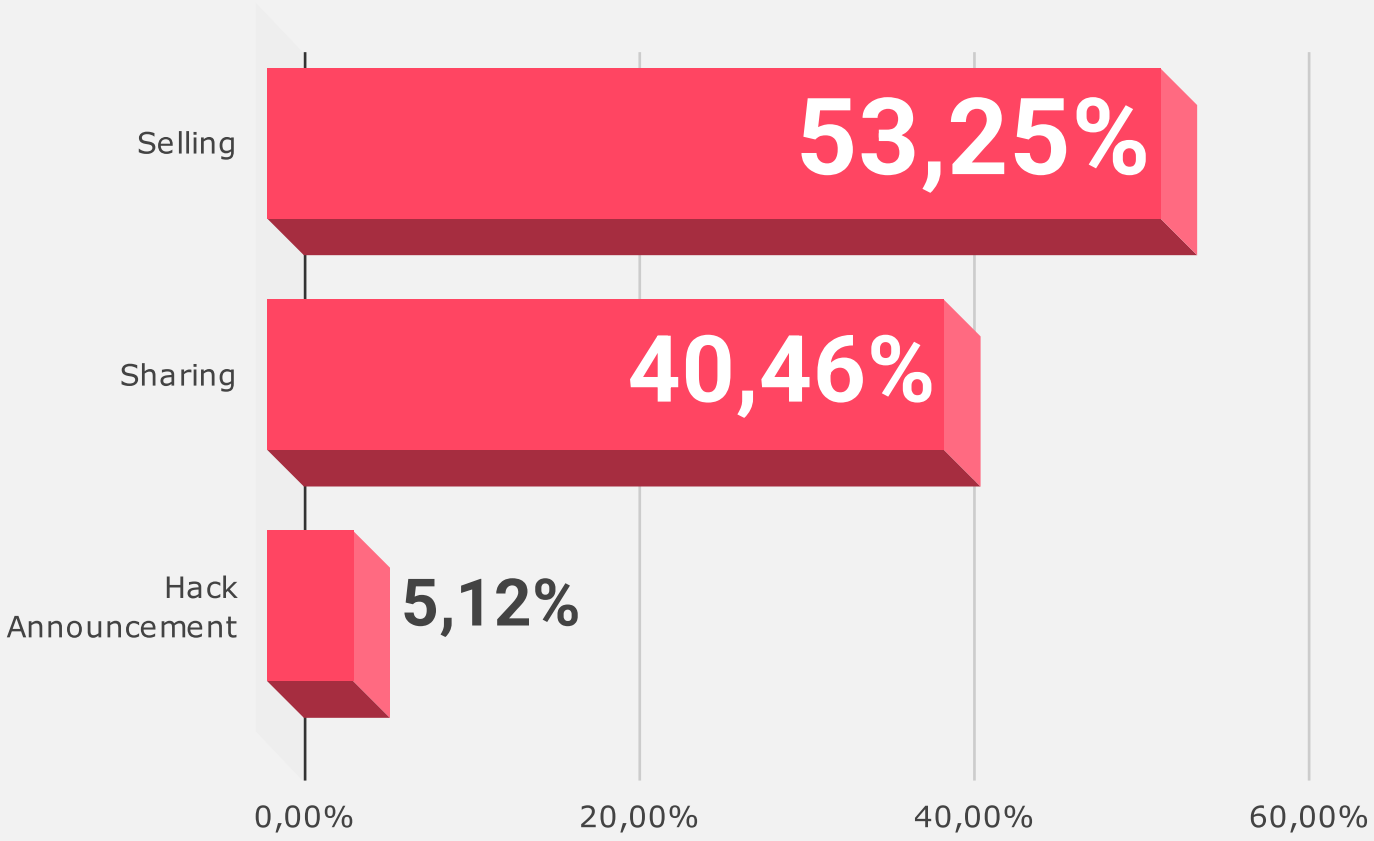
The dataset reveals that nearly 90% of dark web threats and discussions are exclusively focused on the US, indicating a strong, targeted interest in American entities. Only 10.2% of the threats involve both the US and other countries, suggesting that the US remains a primary and independent target in most malicious activities. This underscores the country's high-value status in the eyes of threat actors, likely due to its global economic influence and rich pool of critical infrastructure and data.

Distribution of Dark Web Threats by Industry



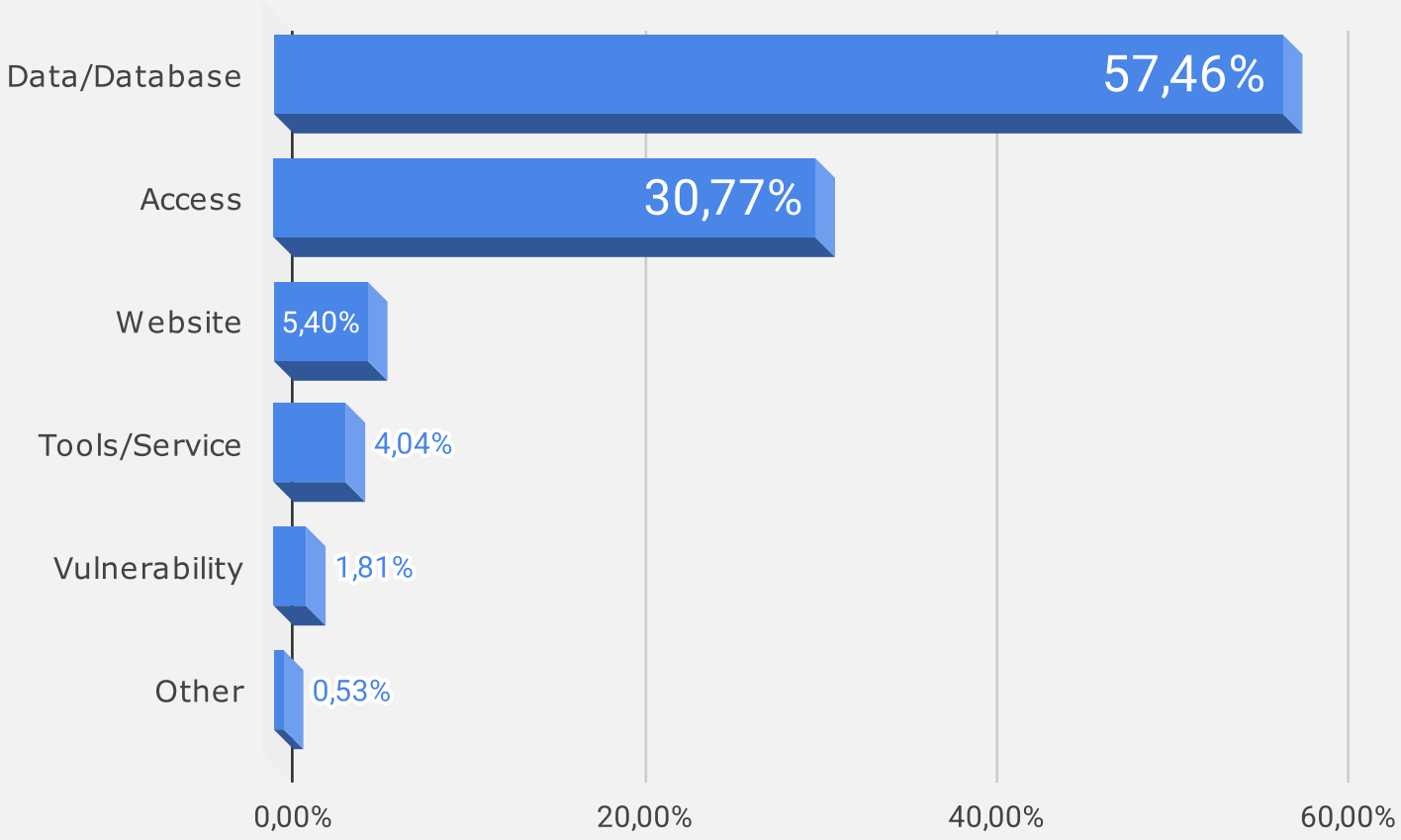
The dataset highlights that the Information sector is the most targeted (11.35%) in dark web activity, followed closely by Finance and Insurance (10.90%) and Public Administration (9.64%). Retail and e-commerce industries also face significant threats, indicating a growing focus on sectors handling large volumes of data and transactions. The presence of Commercial Banking and Healthcare further underlines the targeting of entities with sensitive data or critical infrastructure. This pattern suggests threat actors are prioritizing industries with valuable digital assets or potential for disruption.

Distribution of Dark Web Threats by Threat Categories



The dataset shows that the majority of dark web activity (53.25%) involves selling, likely of data, access, or tools, highlighting a strong cybercrime economy. Sharing-related posts make up 40.46%, suggesting a collaborative environment where threat actors exchange information or resources. Hack announcements are minimal (5.12%), indicating that while attacks are discussed, the primary focus remains on commercial and cooperative exchanges rather than public boasting.

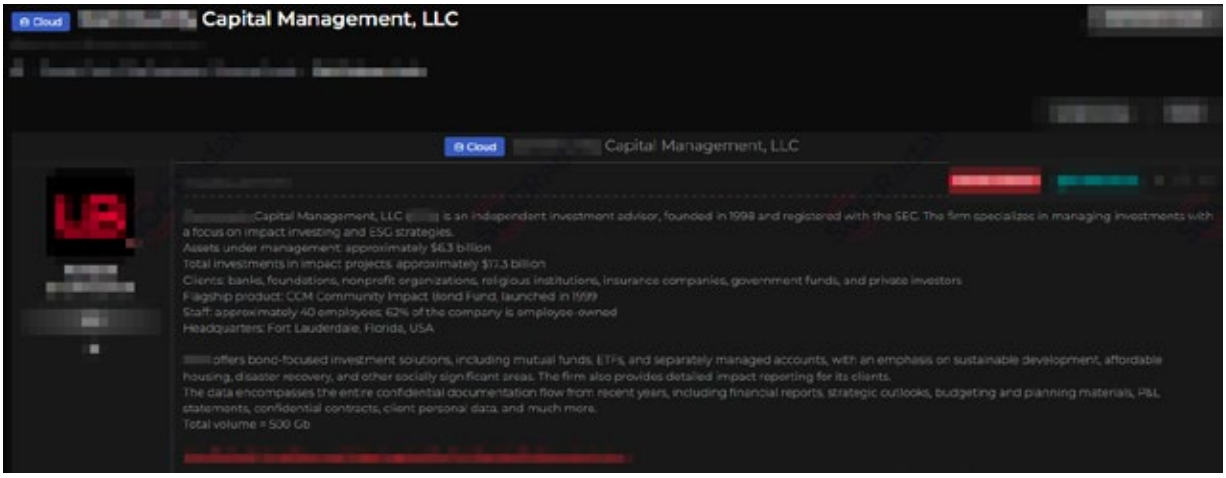
Distribution of Dark Web Threats by Threat Types



The dataset indicates that data breaches and database leaks dominate dark web discussions, accounting for 57.46% of the posts—pointing to a strong market for stolen information. Access-related posts (30.77%) are also significant, often referring to credentials or system entry points for sale. Website targeting, tools/services, and vulnerabilities make up smaller portions, suggesting that while exploitation methods are shared, the main focus remains on data theft and unauthorized access.

Recent Dark Web Activities Targeting the Entities in The US

The Database of a Capital Management Company is Allegedly Leaked



A major data breach targeting a U.S.-based investment advisory firm specializing in impact investing and ESG-focused strategies has been detected on a hacker forum monitored by SOCRadar.

The leaked dataset reportedly includes around 500GB of sensitive materials, encompassing financial reports, strategic outlooks, budgeting documents, profit and loss statements, confidential contracts, and personal information of clients. The firm, which manages approximately $6.3 billion in assets and supports a wide range of institutions such as banks, nonprofits, religious organizations, and government funds, is well-known for its bond-focused sustainable investment products.

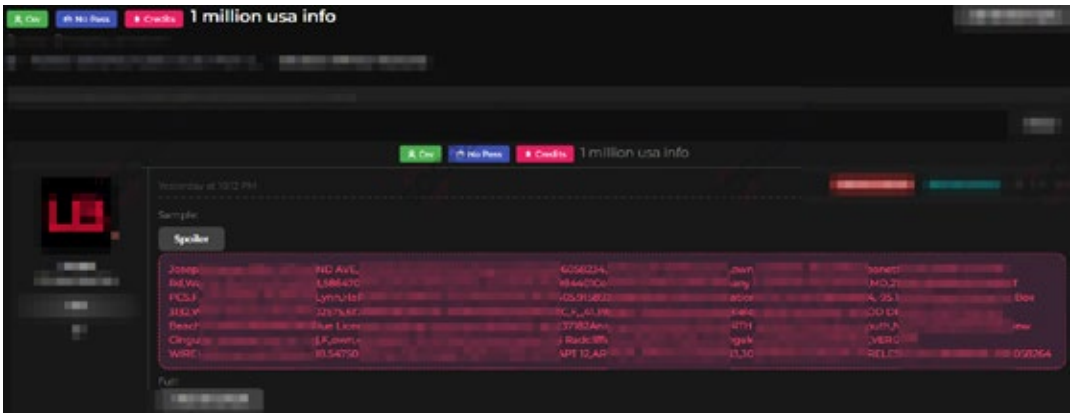
The stolen data appears to span several years and could pose significant risks, given the firm's emphasis on socially responsible investments like affordable housing and disaster recovery initiatives.

The Alleged Database of an American Medical Company is on Sale

A hacker forum monitored by SOCRadar has listed a new alleged database for sale, this time targeting a U.S.-based medical diagnostics provider. The company, which specializes in MRI and high-precision diagnostic services and has been operating for over two decades, is reported to have suffered a breach exposing sensitive patient information.

The leaked data allegedly includes medical records, patient documents, and other confidential files. The database is being offered for $2,000, according to forum listings.

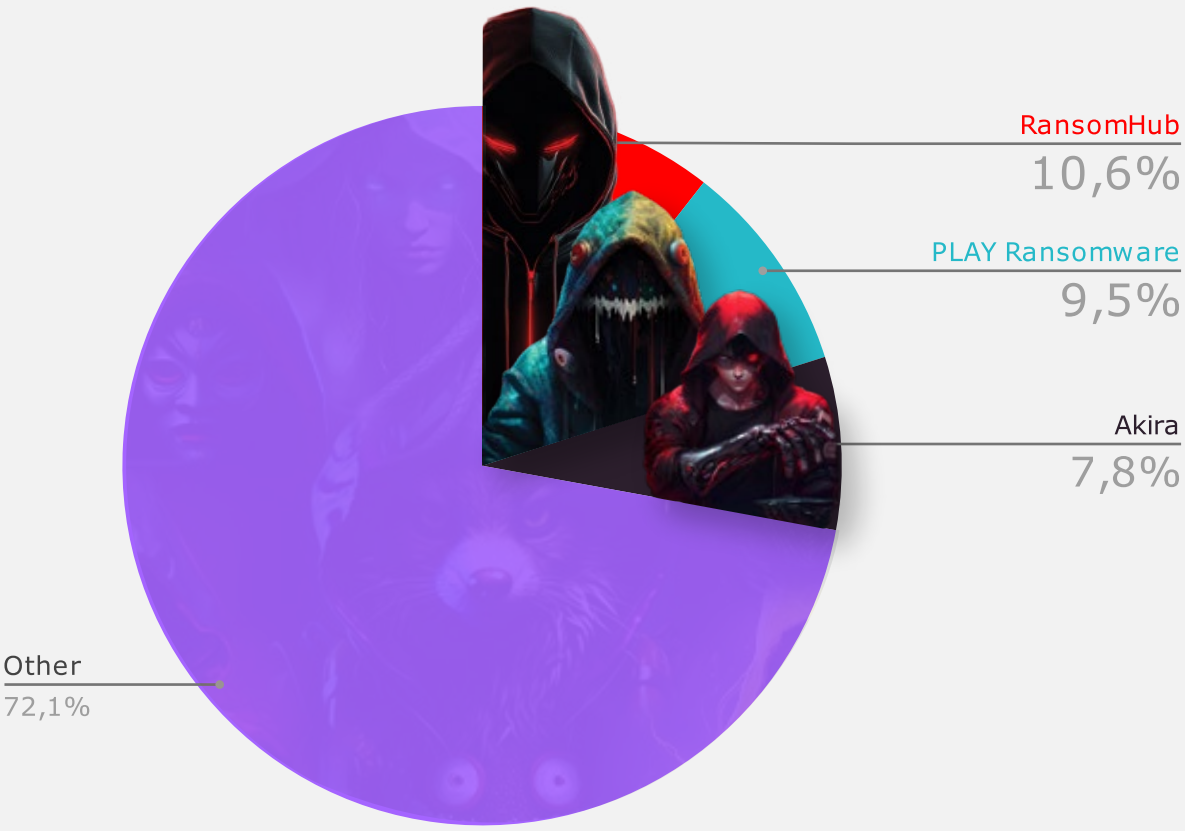
The Alleged Data of American Citizens are Leaked



A dark web forum has surfaced a new alleged data leak targeting American citizens. The exposed dataset reportedly includes sensitive personal details such as names, addresses, numbers, and more.

Ransomware Threats

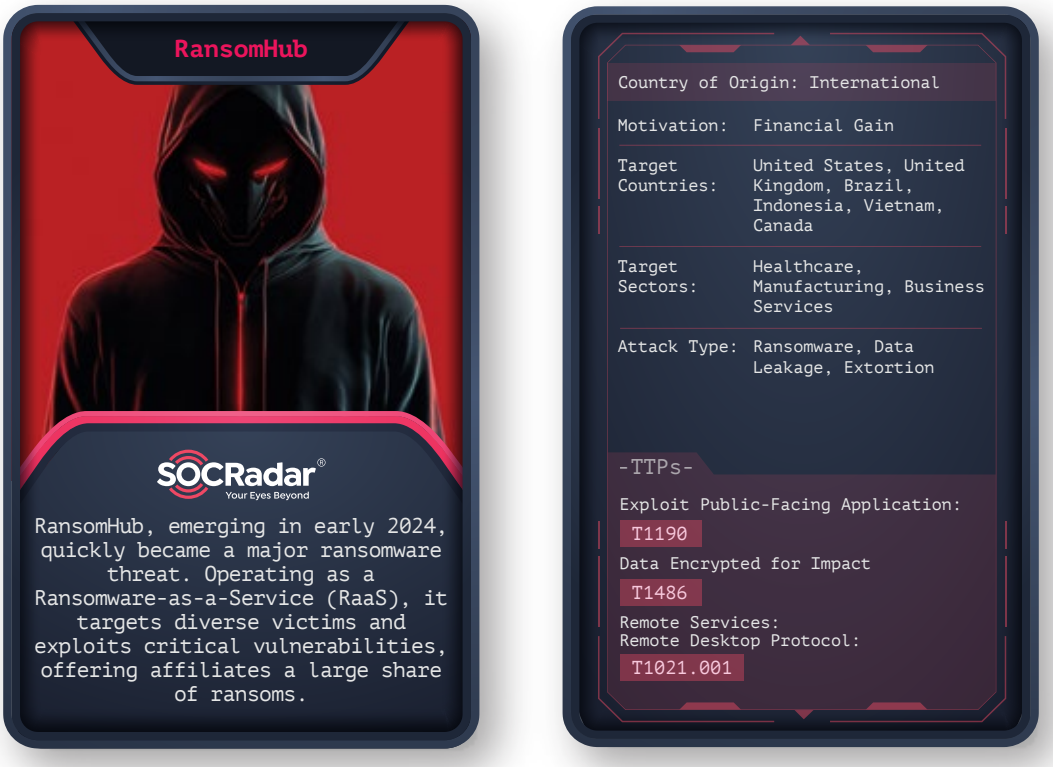
Top Ransomware Groups Targeting The US



The dataset shows that while RansomHub (10.57%), PLAY Ransomware (9.54%), and Akira (7.76%) are the top three groups targeting the US, they collectively account for only about 28% of activity. The remaining 72.13% falls under “Other,” indicating a highly fragmented ransomware landscape with many active groups. This fragmentation complicates defense efforts, as threats stem from a wide array of actors with varying tactics and targets.

A Closer Look into The Top 3 Ransomware Groups

RansomHub



As stated on the group's About page, RansomHub is comprised of hackers from various locations united by a common goal of financial gain. The gang explicitly mentions prohibiting attacks on specific countries and non-profit organizations. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap in targeted companies with other Russian ransomware groups are also worth noting.

You can visit our *blog post* for more detailed information about RansomHub.

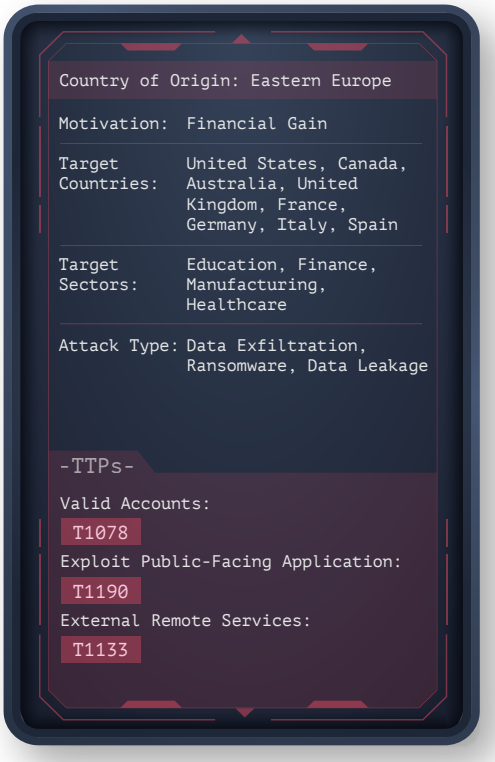
Play Ransomware

Play Ransomware's main target is the Latin American region, and Brazil is at the top of the list. Even though they seem like a new ransomware group, their identified TTPs resemble the Hive and Nokayawa ransomware families. One of the behaviors that makes them look similar is using AdFind, a command-line query tool capable of collecting information from Active Directory.

Double extortion is a widespread technique in which cyber actors threaten to exfiltrate sensitive data. Play Ransomware also uses double extortion against its victims. They can archive the breached data with WinRAR and then upload it to file-sharing sites.

You can visit our *blog post* to read the rest of the threat actor profile.

Akira

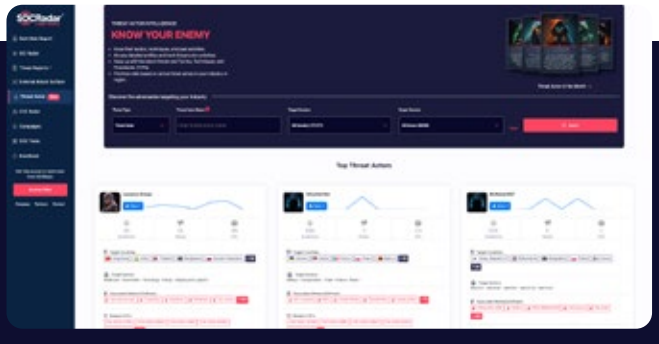


Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

You can visit our *blog post* to read the rest of the threat actor profile.

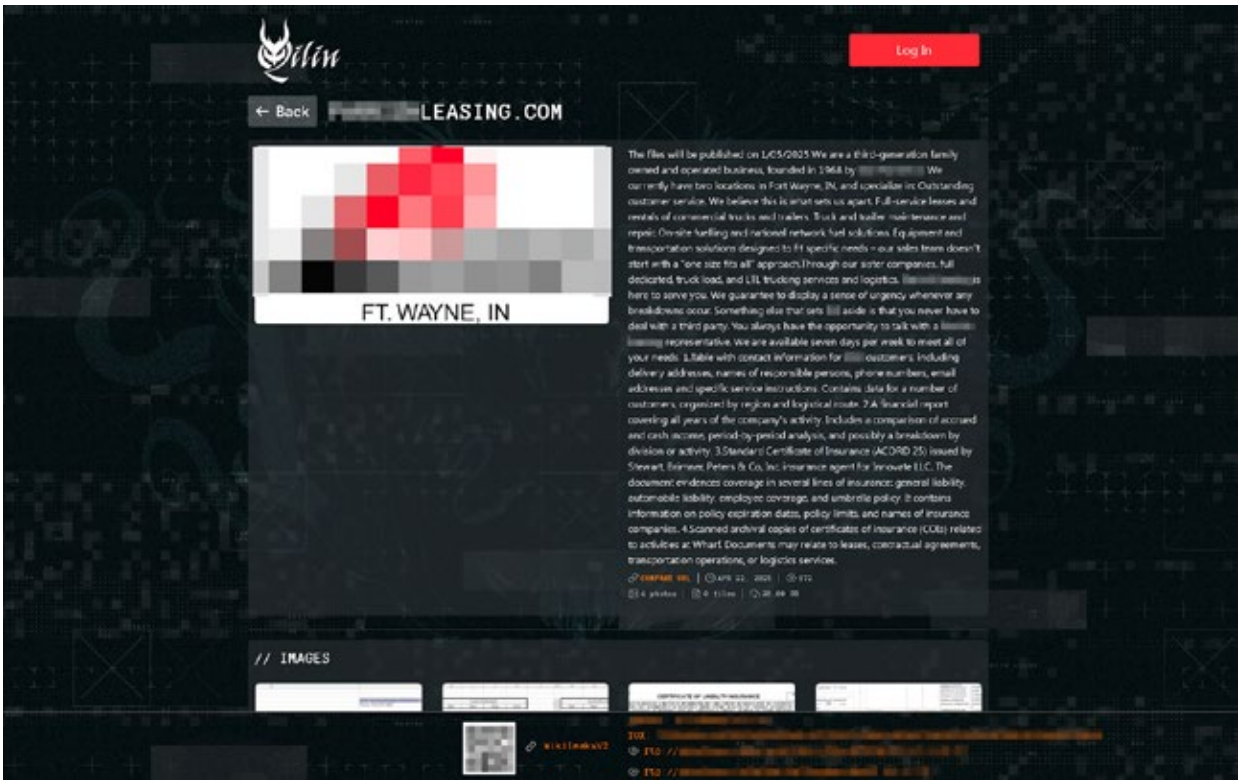


Threat Actor Intelligence Module

SOCRadar enhances cybersecurity measures with its *Threat Actor Intelligence Module*, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.

Recent Ransomware Attacks Targeted Entities in The US

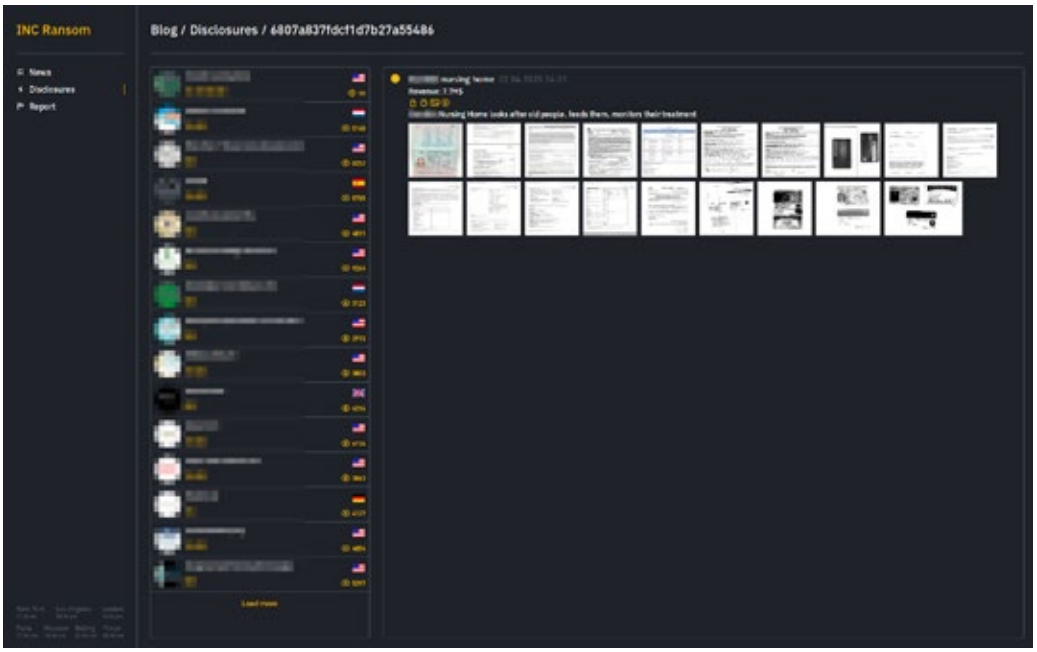
Vehicle Leasing Company Targeted by Qilin Ransomware Group



A ransomware group known as Qilin has listed a new victim on its leak site monitored by SOCRadar.

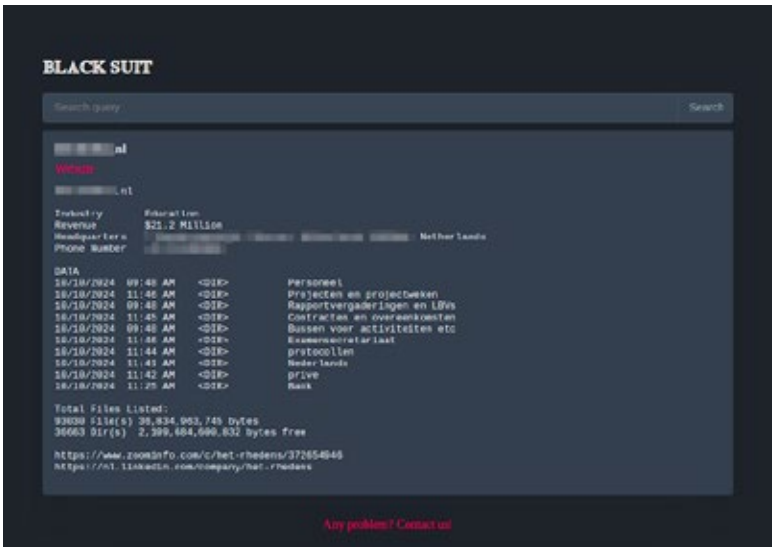
The targeted organization operates in the vehicle leasing and rental services industry and has been in business for several decades, with locations based in Fort Wayne, Indiana. The company, a third-generation, family-owned business founded in 1968, is recognized for its strong emphasis on customer service.

Healthcare Facility Targeted by Ransomware Group



A healthcare provider specializing in elderly care has been listed as a new victim on the ransomware group Incransom's leak site, monitored by SOCRadar. The facility, which offers residential services including medical treatment, daily care, and meal support for seniors, was allegedly compromised in the attack.

Seafood Industry Leader Faces Potential Data Exposure



A major player in the U.S. seafood industry, known for its decades-long history of innovation and diverse product offerings, has reportedly experienced a potential breach involving sensitive internal documents.

Founded in Southern California in 1973, the company has grown from a small operation into one of the nation's largest and most advanced seafood importers and processors.

According to post, private and confidential information including client documents, financial records, payroll data, accounting files, tax information, and personal identification materials may have been exposed.

Stealer Log Statistics

What is a Stealer?

A stealer is a specialized form of malware engineered to exfiltrate sensitive information from infected devices. Stealers operate covertly, maintaining persistence while methodically collecting valuable data. Modern stealers can harvest credentials from browsers, extract cryptocurrency wallet information, capture authentication cookies and collect system information.

What are Stealer Logs?

Stealer logs are the compiled datasets of stolen information from infected devices. These logs typically contain:

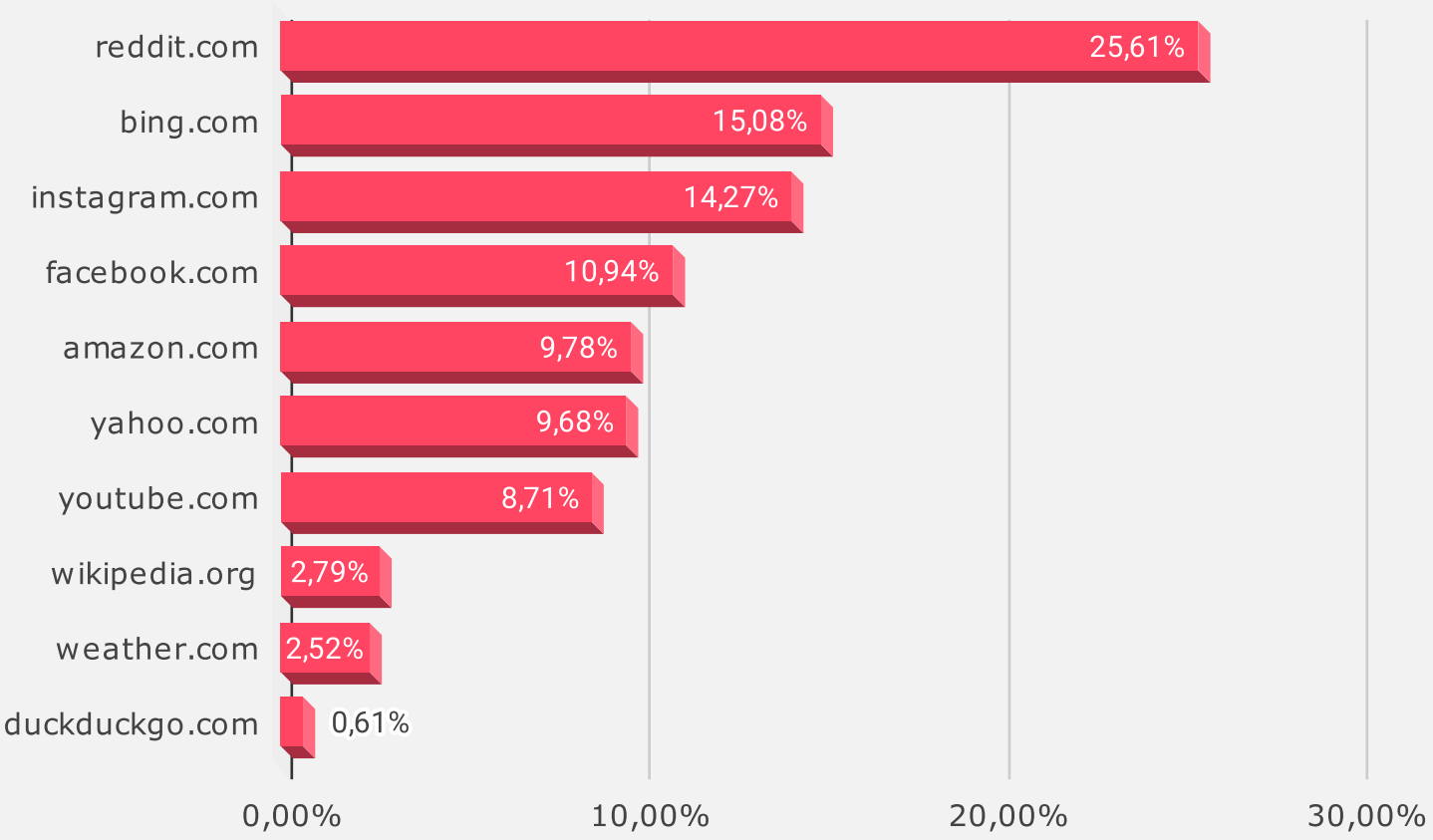
- Browser-saved credentials (usernames and passwords)
- Session cookies and authentication tokens
- Cryptocurrency wallet information and private keys
- Personal information including names, addresses, phone numbers
- Financial data such as credit card information
- System information including hardware specifications, installed software, and IP addresses
- Corporate access credentials including VPN, email, and cloud service logins

Once collected, these logs are either transmitted to command-and-control servers controlled by the threat actors or stored locally for retrieval. Threat actors then either use these logs themselves or sell them on underground marketplaces.

Stealer Log Statistics: Most Visited Domains in The US

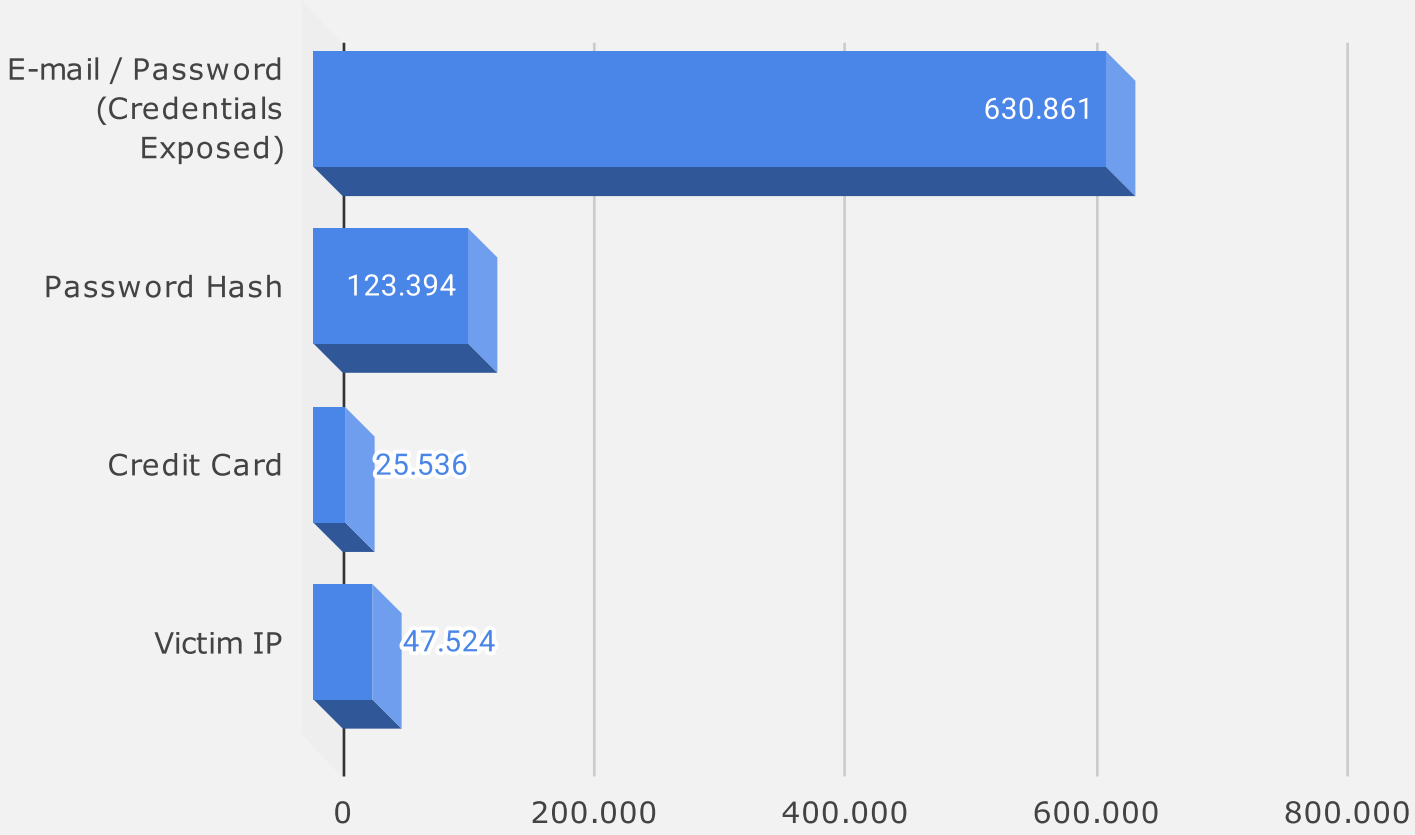
Most Visited Domains
youtube.com
reddit.com
amazon.com
facebook.com
bing.com
duckduckgo.com
yahoo.com
wikipedia.org
instagram.com
weather.com

Stealer Logs - Distribution of the Compromised Data by Domains

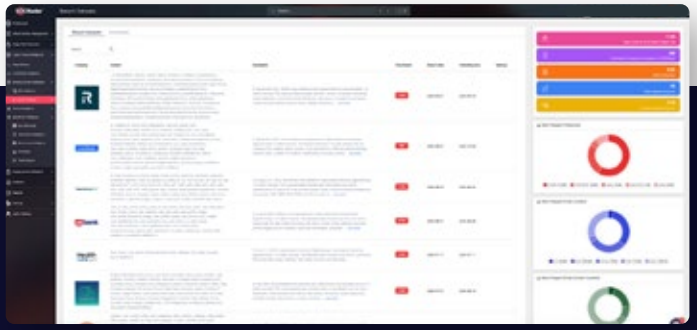


The dataset shows that stealer logs heavily feature credentials and data from reddit.com (25.61%), followed by bing.com (15.08%) and instagram.com (14.27%). Major platforms like Facebook, Amazon, and YouTube are also frequent targets, reflecting attackers' focus on high-traffic, high-value services for maximum exploitation potential. Interestingly, search engines like Bing and DuckDuckGo appear as well, possibly indicating broader browsing session captures rather than specific account targeting.

Stealer Logs - Distribution of the Compromised Data



The dataset reveals a large volume of leaked credentials, with over 630,000 email/password pairs exposed, indicating a major risk for account takeovers. Additionally, 123,394 password hashes were found, suggesting some stolen data originated from partially protected sources. Credit card information (25,536 records) and victim IP addresses (47,524) were also leaked, highlighting the financial and privacy threats posed by stealer malware campaigns targeting users.

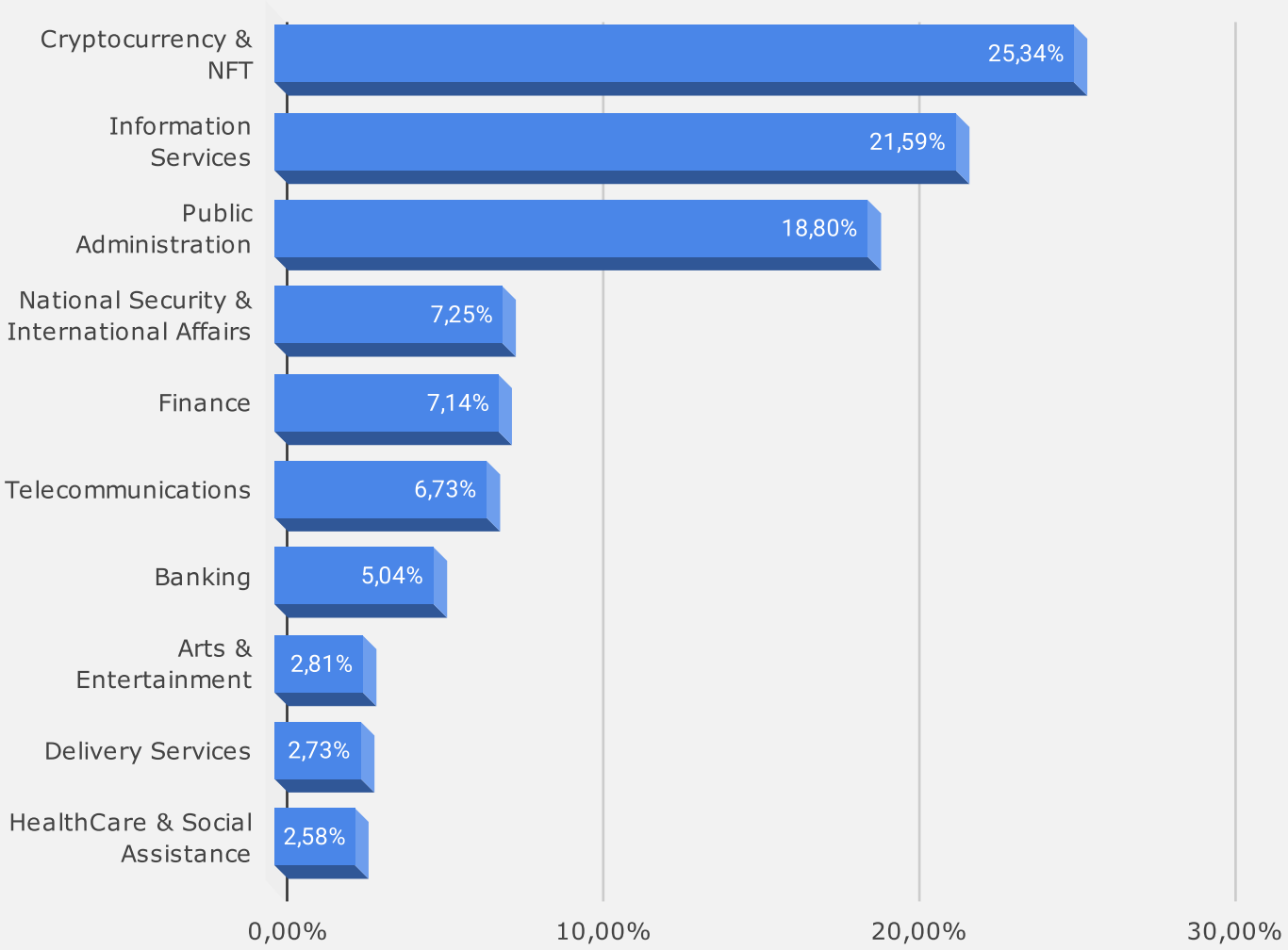


SOCRadar's Identity & Access Intelligence Module

SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

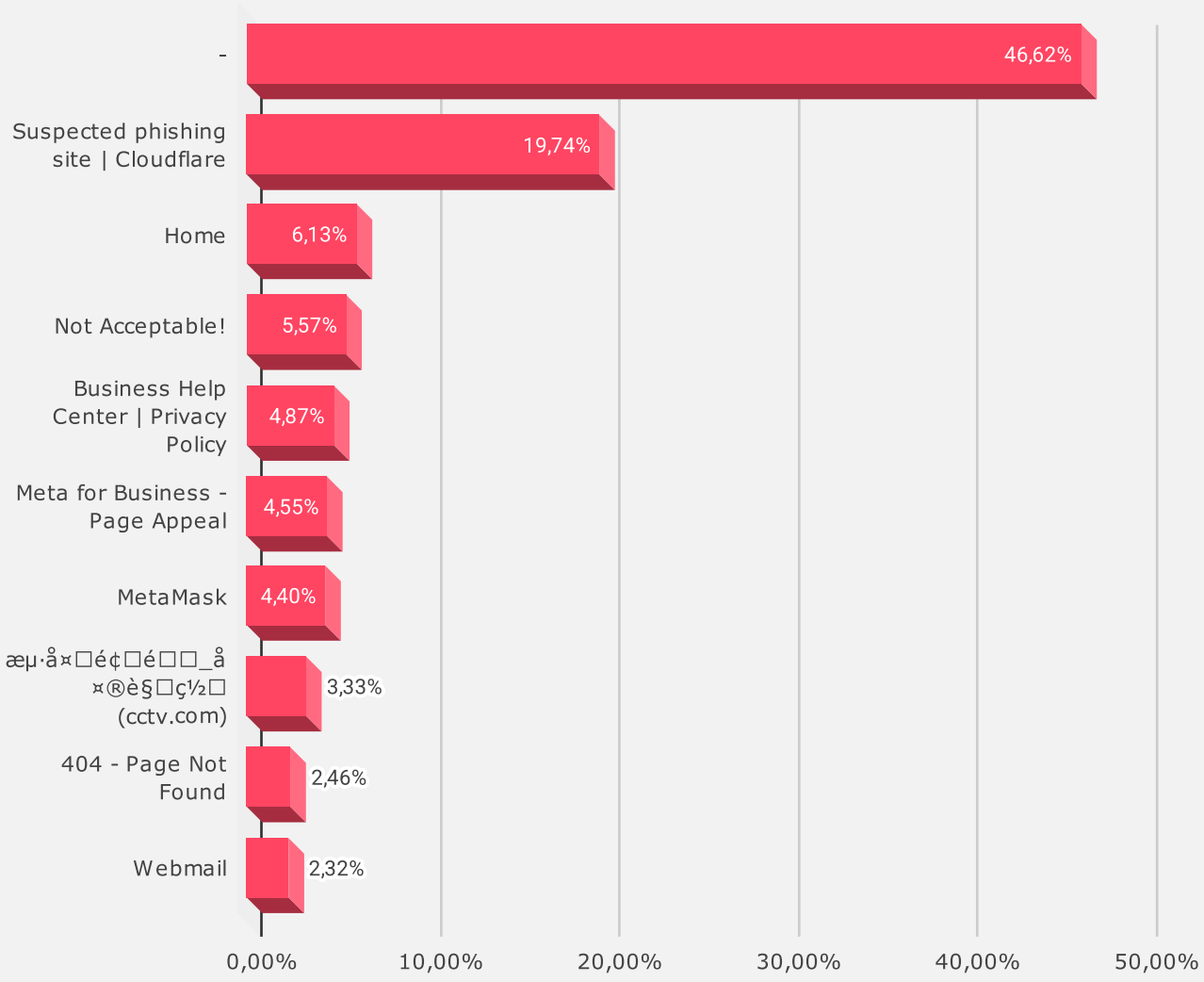
Phishing Threats

Phishing Attacks - Distribution by Industry



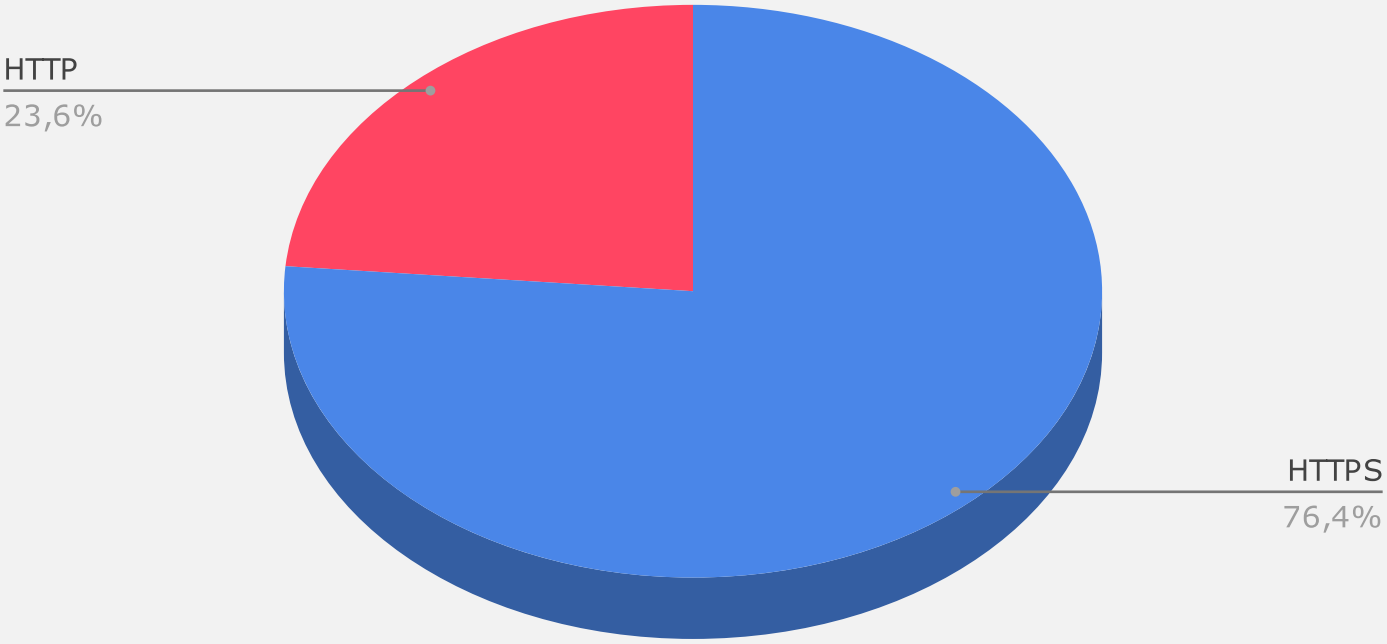
The dataset reveals that phishing attacks in the US are heavily concentrated on Cryptocurrency & NFT platforms (25.34%) and Information Services (21.59%), reflecting attackers' interest in digital assets and data-rich environments. Public Administration (18.80%) also ranks high, indicating persistent attempts to breach government entities. Notably, Finance, Banking, and Telecommunications sectors remain key targets due to their access to sensitive financial and communication data. This distribution suggests that phishing campaigns are strategically aimed at sectors with high-value assets or broad user reach.

Phishing Attacks - Distribution by Phishing Page Title



The dataset shows that 46.62% of phishing pages lack a defined title, a common tactic to evade detection or due to hastily created pages. Notably, 19.74% mimic the Cloudflare phishing warning, possibly to create a false sense of legitimacy. Titles like “Meta for Business”, “MetaMask”, and “Webmail” suggest impersonation of trusted platforms to trick users into divulging credentials. The presence of error-related titles like “404 - Page Not Found” or “Not Acceptable!” may also serve to mislead users or obscure malicious intent.

Phishing Attacks - Distribution by SSL/TLS Protocol



The dataset indicates that 76.4% of phishing sites targeting the US use HTTPS, showing that attackers are increasingly adopting SSL/TLS certificates to make malicious sites appear legitimate and trustworthy. Only 23.6% of phishing sites still use HTTP, highlighting a shift toward encrypted phishing pages. This trend emphasizes that HTTPS alone is no longer a reliable indicator of website safety, and users must rely on additional signals to detect phishing attempts.

DDoS Attack Statistics

- The peak bandwidth witnessed during a DDoS attack reached 941.22 Gbps, highlighting a significant capacity from the cyber threats.
- The highest recorded throughput during these incidents was 540.43 Mpps.
- Most DDoS attacks lasted between 62.52 minutes on average.
- 1.273.975 DDoS attacks were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for the US.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks
ICMP	316,610
TCP ACK	255,553
DNS Amplification	225,187
TCP SYN	203,870
TCP RST	133,539

Lessons Learned: Key Insights and Strategic Recommendations

Strategic Recommendations

- **Invest in Comprehensive Threat Intelligence:** Staying informed about evolving threats and actors enables more proactive defenses.
- **Harden Authentication Mechanisms:** Deploy MFA and encourage password hygiene to protect against credential theft.
- **Enhance Incident Response Capabilities:** Develop and regularly test robust response and recovery plans, particularly for ransomware attacks.
- **Strengthen Employee Awareness:** Security awareness training is essential to combat phishing and social engineering attacks.
- **Collaborate for Greater Resilience:** Share intelligence with industry peers and cybersecurity alliances to stay ahead of emerging threats.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.